

UNITED STATES DISTRICT COURT

for the
District of Oregon

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 3:21-mc-539

The premises and outbuildings located at 455 SW
Walnut Street, Hillsboro, Oregon, more fully described in
Attachment A hereto

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

The premises and outbuildings located at 455 SW Walnut Street, Hillsboro, Oregon, more fully described in Attachment A,
located in the _____ District of _____ Oregon _____, there is now concealed (identify the person or describe the property to be seized):

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 2252A	Transportation, distribution, receipt, possession of, and accessing with the intent to view child pornography

The application is based on these facts:

See the attached affidavit of Special Agent Rebecka E. Brown, Federal Bureau of Investigation.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Rebecka E. Brown, Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
Telephone at 11:08 a.m. (specify reliable electronic means).

Date: 05/07/2021

City and state: Portland, Oregon

Jolie A. Russo

Judge's signature

Honorable Jolie A. Russo, U.S. Magistrate Judge

Printed name and title

STATE OF OREGON)
) ss: AFFIDAVIT OF REBECKA E. BROWN
County of Multnomah)

Affidavit in Support of an Application for a Search Warrant

I, Rebecka E. Brown, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have been so employed for approximately twelve years. I am currently assigned to the FBI's Portland Field Office. As a federal law enforcement officer, I am authorized to investigate and make arrests for violations of federal law, and to apply for federal search warrants. I graduated from the FBI Academy at Quantico, Virginia, after completing a 19-week course of instruction. I have acquired knowledge and information about criminal conduct and investigation from many sources, including formal and informal training, other law enforcement officers, investigators, informants, persons who I have interviewed, and my participation in numerous investigations. I received specialized training in investigating a range of offenses from violent crime to financial crime. I have investigated matters involving the sexual exploitation of children, including the online sexual exploitation of children, particularly as it relates to violations of Title 18, United States Code, Sections 2252A and 2422. I am part of the Portland Child Exploitation Task Force (CETF), which includes FBI Special Agents and Task Force Officers from Portland and Hillsboro, Oregon. The CETF is an intelligence-driven, proactive, multi-agency investigative initiative to combat the proliferation of child pornography/child sexual exploitation facilitated by an online computer. As part of my duties as a federal agent, I work with local, state, and other federal agencies on joint investigations of federal offenses, to include financial crimes.

//

2. I submit this affidavit in support of an application to search the premises and all outbuildings located at **455 SW Walnut Street, Hillsboro, Oregon**, as further described in Attachment A, for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B), which prohibit transporting, distributing, receiving, and possessing child pornography. As set forth below, I have probable cause to believe that such items, further described in Attachment B, are currently located 455 SW Walnut Street, Hillsboro, Oregon.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

4. Title 18, United States Code, § 2252A(a)(1) makes it a crime to knowingly transport child pornography using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer. Section 2252A(a)(2) makes it a crime to knowingly receive or distribute any child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer. Section 2252A(a)(5)(B) makes it a crime to knowingly possess or access with intent to view child pornography that has been mailed, shipped, or transported in

or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that were mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.

5. “Child pornography” is defined in 18 U.S.C. § 2256(8) and includes any visual depiction of a child under the age of 18 years engaged in sexually explicit conduct. “Sexually explicit conduct” is defined under 18 U.S.C. § 2256(2) and includes sexual intercourse, whether genital-genital, oral-genital, anal-genital, or oral-anal; bestiality; masturbation; sadistic or masochistic abuse; and the lascivious exhibition of the genitals or pubic area of any person.

Background on Computers, Digital Devices, and Child Pornography

6. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have drastically changed the manner in which child pornography is produced and distributed.

7. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage.

8. Child pornographers can upload images or video clips directly from a digital camera to a computer. Once uploaded, they can easily be edited, manipulated, copied, and distributed. Paper photographs can be transferred to a computer-readable format and uploaded to a computer through the use of a scanner. Once uploaded, they too can easily be edited, manipulated, copied, and distributed. A modem allows any computer to connect to another computer through the use of a telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

9. The computer's ability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Images and videos of child pornography can also be stored on removable data storage media, such as external hard drives, thumb drives, media cards, and the like, many of which are small and highly portable and easily concealed, including on one's person.

10. The Internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion, including Internet Relay Chat, instant messaging programs, bulletin board services, e-mail, and "peer-to-peer" (P2P) file sharing programs and networks such as Gnutella and BitTorrent, among others. Collectors and distributors of child pornography also use online resources such as "cloud" storage services to store and retrieve child pornography. Such online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

11. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as

temporary files or client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in the computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains P2P software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

12. I know based on my training and experience, and based on conversations I have had with others who investigate child exploitation offenses, that people who have a sexual interest in children, including persons who collect and trade in child pornography, often receive sexual gratification from images and video clips depicting the sexual exploitation of children. They may also use such images and videos to lower the inhibitions of children who they wish to sexually abuse. Such persons maintain their collections of child pornography in safe, secure, and private locations, such as their residence, and on computers and digital storage media under their direct control. Such persons often maintain their collections, which are considered prized possessions, for long periods of time, and prefer not to be without their collections for any prolonged period of time. In some recent cases, however, some persons with a sexual interest in children have been found to download and delete child pornography on a cyclical and repetitive basis, rather than storing a collection of child pornography indefinitely.

13. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of the electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

Background on the BitTorrent Network

14. The BitTorrent network is a popular, publicly available P2P file sharing network. Computers that are part of that network are referred to as “peers” or “clients.” Peers can download files or parts of files from other users while simultaneously providing files or parts of files to others on the network, thereby increasing downloading speed for all of the peers on the network. The BitTorrent network can be accessed through many different client software programs, including the BitTorrent client program, the uTorrent client program, the Vuze client program, and others, all of which are widely available for free on the Internet. The BitTorrent network can be accessed through a laptop or desktop computer, or through a tablet or smartphone device, such as an iPad or iPhone.

15. Files or sets of files are shared on the BitTorrent network through the use of “torrents.” A torrent file is a small file that contains information about the files being shared; including information needed by the client software to locate and download the files but does not contain the files themselves. Torrent files typically contain information such as file name(s), file size(s), file paths, and an “info hash” (a digital fingerprint of sorts for the set of data referenced in the torrent file). The torrent file may also contain information on how to locate the file(s) referenced in the torrent by identifying “trackers.” Trackers are computers on the BitTorrent network that collate information about peers who are sharing the files referenced in the torrent file. A tracker acts as a pointer to peers on the network who are sharing all or part of the files referenced in the torrent but does not actually have the files to be shared.

16. To locate and download files on the BitTorrent network, a user will typically enter keyword searches on a torrent indexing website. Torrent indexing websites are essentially

search engines through which a BitTorrent user can locate torrent files that contain the files or type of files the user wants to download. Once the user locates a torrent file of interest, the user downloads the torrent file to his computer. The user's BitTorrent software client then uses the information in the torrent file to locate other peers on the network that have all or part of the files the user seeks and downloads the files directly from those peers. The downloaded files are then stored in the file folder or storage device designated by the user and remain there until the user moves or deletes them. Once a user downloads files (or parts of files), other users on the BitTorrent network can download those files (or parts of files) from that user, as long as the files remain in the folder/storage device designated by the user.

17. Law enforcement agents can search the BitTorrent network in much the same way in order to locate individuals who are offering to share files containing images or videos of child pornography. Law enforcement agents can search for torrents known to contain images or videos of child pornography and can download the files described in those torrents using client software designed to download only from a single source at a single IP address.

Statement of Probable Cause

Benton County Investigation of IP address 73.157.162.10

18. On March 8, 2021, a detective from the Benton County Sheriff's Office verified that a computer running undercover investigative software made multiple direct connections to a device at IP address 73.157.162.10 between 04/29/2020 and 02/23/2021. Multiple partial and complete files were successfully downloaded from the suspect device. The suspect device was the sole candidate for each download, and as such, each file was downloaded directly from the suspect device. The detective reviewed several of these files and found that many contained

sexually explicit conduct involving a child. At my request, the Benton County Sheriff's Office sent encrypted copies of the downloaded files to the Portland FBI Office.

FBI Investigation

19. On March 10, 2021, I downloaded and extracted approximately 35GB of data that the Benton County Sheriff's Office downloaded from IP address 73.157.162.10. Many of these files depicted child exploitative material including infants, toddlers, and other children being sexually assaulted by adults. Descriptions of three of these files are as follows:

File: \cpack3_little_joys\webcams\sets\Brunette girl on Skype\Video_2012-11-09_202752.wmv

Date: January 27, 2021, at 7:11 UTC

Description: A 1m53s video of a prepubescent girl, approximately eight to ten years old, nude from the waist down, wearing a blue and white graphic shirt and white socks. The girl is sitting on a chair with her legs spread apart facing a camera. Throughout the video, the girl inserts her fingers and a small cylindrical object into her anus.

File: \downloads\G39\Set 39\Gracel_Set39_068.jpg

Date: February 22, 2021, at 12:49 UTC

Description: An approximately 39 second video of a four- to five-year-old girl wearing a pink Winnie The Pooh shirt sitting on a bed. A nude adult male with an erect penis is standing in front of her. The adult male instructs the girl to hold his penis, which she does, before moving aside to adjust the camera. When the man returns, he tells the girl to look at the camera while she licks his penis.

File: \downloads\Baby fucked\Pict02__055.jpg

Date: February 23, 2021, at 11:47 UTC

Description: Inside the folder "Baby fucked" was a series of 42 images of an infant girl being sexually abused by an adult male. In several images that show part of the child's face, her expression suggests that she is distressed by the abuse. In one of these images, the female infant, who is wearing a yellow shirt with a cartoon penguin on it, is laying on what appears to be a mattress. An adult male is forcing the tip of his erect penis into her vagina. The child's groin and stomach are smeared with a white fluid substance that appears to be ejaculate.

20. On March 12, 2021, the FBI issued a subpoena to Comcast Communications (Comcast) for subscriber information associated with the following IP address: 73.157.162.10 at the following dates/times:

01/27/2021 at 7:11 UTC

02/22/2021 at 12:49 UTC

02/23/2021 at 11:47 UTC

21. On March 17, 2021, Comcast responded to the request and provided the following subscriber information:

Subscriber Name: CLAYTON THOMPSON

Service Address: 455 SW WALNUT ST, HILLSBORO, OR

Account Status: Active

Accurint queries conducted in March 2021, suggested that Clayton THOMPSON (DOB XX/XX/1987) may reside at 455 SW Walnut Street with his wife, Katelyn Thompson.

22. On March 18, 2021, a physical surveillance was conducted at 455 SW Walnut Street, Hillsboro, Oregon. The residence is a single-story structure on a corner lot with beige colored siding and beige trim. The front door is south facing and is darker beige. A small porch covers the front entrance; the numbers, "455," are affixed to a porch support. A beige-colored shed is situated towards the rear of the residence on the west side. A white Ford Escape bearing Oregon (OR) license plate 727JXS was parked in the driveway of the residence. A red Buick bearing OR license plate 875FLY was parked on the west side of the residence just off SW Dennis Avenue. Oregon Department of Motor Vehicles (DMV) reported the following information for the two vehicles:

1996 Buick Century, four-door, 875FLY

R/O: Clayton Deloy Thompson

Address: 4050 Liberty Rd S Apt 14, Salem, OR

2015 Ford Escape, four-door, 727JXS
R/O: Rexius Forest by Products Inc
Address: 1275 Bailey Hill Rd, Eugene, OR

23. A WiFi survey taken directly in front of the residence revealed that all visible SSID's were encrypted/password protected. One SSID was named, "Thompson," which is the last name of the subscriber reported by Comcast.

24. An NCIC query for Clayton THOMPSON on March 18, 2021, revealed several arrest records for Driving Under the Influence (DUI) in 2007 and unlawful possession of marijuana in 2010. NCIC was negative for Katelyn Thompson.

Examination of Data Storage Devices

25. I know that a forensic image is an exact physical copy of a data storage device. A forensic image captures all data on the subject media without viewing or changing the data in any way. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of data for information subject to seizure pursuant to the warrant.

26. Since digital data may be vulnerable to inadvertent modification or destruction, a controlled environment, such as a law enforcement laboratory, is often essential to conducting a complete and accurate analysis of the digital devices from which the data will be extracted. Software used in a laboratory setting can often reveal the true nature of data. Therefore, a computer forensic reviewer needs a substantial amount of time to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or an instrumentality of a crime.

27. Analyzing the contents of a computer or other electronic storage device, even without significant technical difficulties, can be very challenging, and a variety of search and analytical methods must be used. For example, searching by keywords, which is a limited text-based search, often yields thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process. The computer may have stored information about the data at issue which may not be searchable text, such as: who created it; when and how it was created, downloaded, or copied; when it was last accessed; when it was last modified; when it was last printed; and when it was deleted. The relevance of this kind of data is often contextual. Furthermore, many common email, database, and spreadsheet applications do not store data as searchable text, thereby necessitating additional search procedures. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted, or printed data requires a search of events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which users logged in, whether users shared passwords, whether a computer was connected to other computers or networks, and whether the users accessed or used other programs or services in the relevant time period, can help determine who was sitting at the keyboard.

28. *Latent Data:* Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence and to recover latent data. The recovery of such data may require the use of special software and procedures. Data that represents electronic files or remnants of such files can be recovered months or even years after it has been downloaded onto a hard drive, deleted, or viewed via the Internet. Even when such

files have been deleted, they can be recovered months or years later using readily available forensic tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in space on the hard drive or other storage media that is not allocated to an active file.

29. *Contextual Data*

a. In some instances, the computer “writes” to storage media without the specific knowledge or permission of the user. Generally, data or files that have been received via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to such data or files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve artifacts of electronic activity from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer usage. Logs of access to websites, file management/transfer programs, firewall permissions, and other data assist the examiner and investigators in creating a “picture” of what the computer was doing and how it was being used during the relevant time in question. Given the interrelationships of the data to various parts of the computer’s operation, this information cannot be easily segregated.

b. Digital data on the hard drive that is not currently associated with any file may reveal evidence of a file that was once on the hard drive but has since been deleted or edited, or it could reveal a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard

drive that show what tasks and processes on the computer were recently used. Web browsers, email programs, and chat programs store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence.

c. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be learned from the absence of particular data on a digital device. Specifically, the lack of computer security software, virus protection, and malicious software, evidence of remote control by another computer system, or other programs or software may assist in identifying the user indirectly and may provide evidence excluding other causes for the presence or absence of the items sought by this application. Additionally, since computer drives may store artifacts from the installation of software that is no longer active, evidence of the historical presence of the kind of software and data described may have special significance in establishing timelines of usage, confirming the identification of certain users, establishing a point of reference for usage and, in some cases, assisting in the identification of certain users. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Such data may also lead to exculpatory evidence. Evidence of the absence of particular data on the drive is not generally capable of being segregated from the rest of the data on the drive.

Search Procedure

30. This application seeks permission to search for particular items, described in Attachment B, which will likely be found in the residence described in Attachment A, in whatever form those items may be found. One form in which that evidence will likely be found is as data stored on a computer's hard drive, on other digital storage media, or on other digital devices, including cell phones. Thus, the warrant applied for would authorize the seizure of electronic storage media or the copying of electronically stored information, all under Fed. R. Crim. P. 41(e)(2)(B).:

31. Specifically, this application seeks permission to search for, seize, and examine:

- a. All records, documents, or materials, including correspondence, pertaining to the production, transportation, distribution, receipt, or possession of child pornography, as that term is defined in 18 U.S.C. § 2256;
- b. All originals and copies of visual depictions of minors engaging in sexually explicit conduct as that term is defined in 18 U.S.C. § 2256, including photographs, images, and videos, whether in physical or digital form;
- c. Computers, storage media, or digital devices, including cellular telephones, that were used or are capable of being used to commit the offenses described above, or to create, access, or store contraband or evidence, fruits, or instrumentalities of those offenses;
- d. Evidence of Internet usage for the transportation, distribution, receipt, or possession of child pornography as defined in 18 U.S.C. § 2256, including dates and times of usage; IP addresses; and screennames, user names, and passwords used to access

the Internet or any accounts via the Internet;

e. Communications, including emails, chats, bulletin board posts, and comments. relating to the production, transportation, distribution, receipt, or possession of child pornography, to children engaged in sexually explicit conduct, and/or to a sexual interest in children; and

f. All records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as that term is defined in 18 U.S.C. § 2256.

g. “Records,” “items,” “documents,” and “materials” include all of the foregoing items in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

32. I have probable cause to believe that the items described in Attachment B will be stored on one or more digital device(s), based on the foregoing facts and on my knowledge, training, and experience that:

a. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person “deletes” a file on a digital device, the data contained in the file does not actually disappear; rather, that data remains on the digital device until it is overwritten by new data. Therefore, deleted files or remnants of deleted

files may reside in free space or slack space – that is, in space on the digital device that is not currently being used by an active file – for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

b. Wholly apart from user-generated files, digital devices – in particular, internal hard drives – contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. For example, forensic evidence can take the form of operating system configurations, artifacts from the operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Digital device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

33. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant but also forensic electronic evidence that establishes how digital devices were used, the purpose of their use, who used them, and when. I have probable cause to believe that this forensic electronic evidence will be on any digital device in the residence described in Attachment A, because, based on my knowledge, training, and experience, I know:

a. Data on a digital device can provide evidence of a file that was once on the digital device but has since been deleted or edited, or of a deleted portion of a file

(such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the digital device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such “timeline” information allows the forensic analyst and investigators to understand the chronological context of access to the digital device, its use, and events relating to the offense under investigation. This “timeline” information may tend to either inculcate or exculpate the user of the digital device. In addition, forensic evidence on a digital device may provide relevant insight into the user’s state of

mind as it relates to the offense under investigation. For example, information on a digital device may indicate the user's motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a "wiping program" to destroy evidence on the digital device, or password-protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the digital device and the application of knowledge about how a digital device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular

thing is not present on a digital device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a digital device to commit a crime such as the child pornography offenses described herein, the individual's digital device will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of the crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

34. Specifically, this application seeks permission to search for, seize, and examine, for any computer or storage medium whose seizure is otherwise authorized by the warrant and any computer, storage medium, or digital device that contains, is capable of containing, or in which is stored records or information that is otherwise called for by this warrant and

Attachment B (hereinafter "Computer"):

a. Evidence of who used, owned, or controlled the Computer at the time the things described in this warrant and Attachment B were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs,

photographs, and correspondence;

b. Evidence of software that would allow others to control the Computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. Evidence of the lack of such malicious software;

d. Evidence indicating how and when the Computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime under investigation and to the Computer user;

e. Evidence indicating the Computer user's state of mind as it relates to the crime under investigation;

f. Evidence of the attachment to the Computer of other storage devices or similar containers for electronic evidence;

g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer;

h. Evidence of the times the Computer was used;

i. Passwords, encryption keys, and other access devices that may be necessary to access the Computer;

j. Documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer;

k. Records of or information about IP addresses used by the Computer;

l. Records of or information about the Computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"

web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. Contextual information necessary to understand the evidence described in this warrant and Attachment B; and

n. Routers, modems, and network equipment used to connect computers to the Internet.

35. In most cases, a thorough search of premises for information that might be stored on a digital device often requires the seizure of the device and a later, off-site review consistent with the warrant. In lieu of removing a digital device from the premises, it is sometimes possible to image or copy it. Generally speaking, imaging is the taking of a complete electronic picture of the digital device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the digital device and to prevent the loss of the data either from accidental or intentional destruction. This is true because:

a. Not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine digital devices to obtain evidence. Digital devices can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be

impractical and invasive to attempt on-site.

b. Records sought under this warrant could be stored in a variety of formats that may require off-site reviewing with specialized forensic tools. Similarly, digital devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

36. *Nature of the examination.* Based on the foregoing, and consistent with Fed. R. Crim. P. 41(e)(2)(B), the warrant for which I am applying would permit seizing, imaging, or otherwise copying digital devices that reasonably appear to contain some or all of the evidence described in the warrant and Attachment B, and would authorize a later review of the device or information consistent with the warrant. The later review may require techniques, including computer-assisted scans of the entire device that might expose many parts of a hard drive to human inspection in order to determine whether it contains material subject to seizure and search under the warrant.

37. Law enforcement personnel will use procedures designed to identify items to be seized under the warrant. These procedures may include the use of a “hash value” library to exclude normal operating system files that do not need to be searched. In addition, law enforcement personnel may search for and attempt to recover deleted, hidden, or encrypted data

to determine whether the data falls within the list of items to be seized under the warrant.

38. Law enforcement personnel will perform an initial search of the digital devices within a reasonable amount of time not to exceed 120 days from the date of the execution of the warrant. If, after the initial search, law enforcement personnel determine that an original device contains any data falling within the list of items to be seized pursuant to this warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of the chain of custody, and resolve any issues regarding contamination of the evidence. If the government needs additional time to determine whether a digital device contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date of the execution of the warrant. The government shall complete the search of the digital devices within 180 days of the date of execution of the warrant. If the government needs additional time to complete the search, it may seek an extension of the time period from the Court.

39. If, at the conclusion of the search, law enforcement personnel determine that particular files or file folders on a digital device do not contain any data falling within the list of items to be seized pursuant to the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the list of items to be seized pursuant to the warrant, as well as data within the operating system, file system, or software application relating or pertaining to files or data falling within the list of items to be seized pursuant to the warrant (such as log files, registry data, and the like), through the conclusion of the case.

40. If a digital device does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will return that original data device to its owner within a reasonable period of time following the search of that device, and will seal any image of the device, absent further authorization from the Court.

41. The government may retain any digital device containing contraband or evidence, fruits, or instrumentalities of the offenses described herein, or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

41. The government has made no prior efforts in other judicial fora to obtain the evidence sought in this warrant.

Retention of Image

42. The government will retain a forensic image of the electronic storage device subjected to analysis for a number of reasons, including proving the authenticity of evidence to be used at trial; responding to questions regarding the corruption of data; establishing the chain of custody of data; refuting claims of fabricating, tampering with, or destroying data; and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Inventory and Return

43. With respect to the seizure of electronic storage media or the seizure or imaging of electronically stored information, the search warrant return to the Court will describe the physical storage media that were seized or imaged.

Conclusion

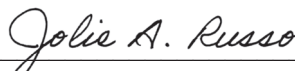
44. Based on the foregoing information, I have probable cause to believe that

contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B), as set forth herein and in Attachment B, are currently at the premises and all outbuildings located at 455 SW Walnut Street, Hillsboro, Oregon, more fully described in Attachment A. I therefore request that the Court issue a warrant authorizing a search of the residence described in Attachment A for the items described above and in Attachment B, and the seizure and examination of any such items found.

45. This affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorneys (AUSA) Natalie Wight and Andrew Ho prior to being submitted to the Court. AUSAs Wight and Ho advised me that in their opinion, the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

REBECKA E. BROWN
Special Agent
Federal Bureau of Investigation

Sworn via telephone pursuant to Fed. R. Crim. P. 4.1(b) at 11:08 A.M. this 7th day of May 2021.



THE HONORABLE JOLIE A. RUSSO
United States Magistrate Judge

ATTACHMENT A

Description of Location to be Searched

The Premises and Outbuildings Located at 455 SW Walnut Street, Hillsboro, Oregon

The premises located at 455 SW Walnut Street, Hillsboro, Oregon, is a single-story structure on a corner lot with beige colored siding and beige trim. The front door is south facing and is darker beige. A small porch covers the front entrance; the numbers, “455,” are affixed to a porch support. A beige-colored shed is situated towards the rear of the residence on the west side.



ATTACHMENT B

Items to Be Seized

The following records, documents, and items that constitute contraband and evidence, fruits, and/or instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(1), (a)(2), and (a)(5)(B), involving the transportation, distribution, receipt, and possession of child pornography.

1. Items to be searched for, seized, and examined:
 - a. All records, documents, or materials, including correspondence, pertaining to the production, transportation, distribution, receipt, possession of, or accessing with intent to view child pornography, as that term is defined in 18 U.S.C. § 2256;
 - b. All originals and copies of visual depictions of minors engaging in sexually explicit conduct as that term is defined in 18 U.S.C. § 2256, including photographs, images, and videos, whether in physical or digital form;
 - c. Computers, storage media, or digital devices, including cellular telephones, that were used or are capable of being used to commit the offenses described above, or to create, access, or store contraband or evidence, fruits, or instrumentalities of those offenses;
 - d. Evidence of internet usage for the transportation, distribution, receipt, possession of, or accessing with intent to view child pornography as defined in 18 U.S.C. § 2256, including dates and times of usage; IP addresses; and screennames, user names, and passwords used to access the internet or any accounts via the internet;
 - e. Communications, including emails, chats, bulletin board posts, and

comments relating to the production, transportation, distribution, receipt, possession of, or accessing with the intent to view child pornography, to children engaged in sexually explicit conduct, and/or to a sexual interest in children; and

f. All records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as that term is defined in 18 U.S.C. § 2256.

2. As used in this attachment, the terms “records,” “items,” “documents,” and “materials” include all of the foregoing items in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant and any computer, storage medium, or digital device that contains, is capable of containing, or in which is stored records or information that is otherwise called for by this warrant (hereinafter “Computer”):

a. Evidence of who used, owned, or controlled the Computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

b. Evidence of software that would allow others to control the Computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

- c. Evidence of the lack of such malicious software;
- d. Evidence indicating how and when the Computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime under investigation and to the Computer user;
- e. Evidence indicating the Computer user's state of mind as it relates to the crime under investigation;
- f. Evidence of the attachment to the Computer of other storage devices or similar containers for electronic evidence;
- g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer;
- h. Evidence of the times the Computer was used;
- i. Passwords, encryption keys, and other access devices that may be necessary to access the Computer;
- j. Documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer;
- k. Records of or information about Internet Protocol addresses used by the Computer;
- l. Records of or information about the Computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. Contextual information necessary to understand the evidence described in

this attachment; and

n. Routers, modems, and network equipment used to connect computers to the Internet.

Search Procedure

4. The search for data capable of being read, stored, or interpreted by a computer or storage device may require authorities to employ techniques, including imaging any computer or storage media and computer-assisted scans and searches of the computers and storage media, that might expose many parts of the computer to human inspection in order to determine whether it constitutes evidence as described by the warrant.

5. The initial examination of the computer and storage media will be performed within a reasonable amount of time not to exceed 120 days from the date the warrant is executed. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date the warrant is executed. The government shall complete this review within 180 days of the date the warrant is executed. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

6. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the computer and storage media do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within

the scope of the warrant, through the conclusion of the case.

7. If an examination is conducted and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the computer and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

8. The government may retain any digital device containing contraband or evidence, fruits, or instrumentalities of the offenses described herein, or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

9. The government will retain a forensic image of the computer and storage media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering with, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.